



SANGFOR

CCOM

Panduan Konfigurasi Cyber Command dan Endpoint Secure

Versi 3.0.48

Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Desember 2020	Panduan Konfigurasi Cyber Command dan Endpoint Secure.

Daftar Isi

Bab 1 Skenario Penerapan	2
Bab 2 Panduan Konfigurasi	2
2.1 Endpoint Secure terhubung ke Cyber Command	2
2.2 Correlated Block	4
2.3 Access Control	4
2.4 Threat Scan	5
2.5 Forensics.....	6

Bab 1 Skenario Penerapan

Dokumen ini sebagian besar memperkenalkan hubungan konfigurasi dan fungsi utama dari Cyber Command dengan Endpoint Secure. Berikut ini adalah rincian fungsi dari Cyber Command correlated dengan Endpoint Secure.

- (1) Endpoint Secure dapat memberikan semua informasi asset ke Cyber Command.
- (2) Endpoint Secure dapat memberikan catatan perihal keamanan ke Cyber Command.
Catatan perihal keamanan sebagian besar mencakup perihal Virus, perihal Webshell, perihal Brute force, perihal Botnet dan catatan akses Micro Segmentation.
- (3) Correlated block digunakan untuk memblokir akses ke atau dari endpoint dengan alamat IP tertentu. Cyber Command dapat terhubung dengan Endpoint Secure untuk mengisolasi atau memblokir sebuah endpoint ketika perihal keamanan terdeteksi.
- (4) Access control hampir sama dengan correlated block, tapi access control dapat memblokir akses keluar dan masuk ke endpoint di semua port yang ditentukan, membuatnya lebih terperinci dari correlated block. Access control dapat mencegah ancaman keamanan, dan setelah ancaman keamanan terdeteksi, kalian dapat dengan cepat memblokir akses endpoint tanpa mempengaruhi operasi sistem bisnis.
- (5) Threat scan mengacu pada melakukan full scan atau quick scan pada endpoint yang beresiko. Jika sebuah endpoint terinfeksi, correlated Endpoint Secure dapat melakukan pendeteksian virus dan menghapus berkas yang terinfeksi.
- (6) Forensics mengacu ke proses mengumpulkan bukti yang mana endpoint beresiko mengunjungi botnet domain yang berbahaya. Bukti termasuk proses nama, detail proses, dsb. Forensic secara khusus berguna ketika berkas virus susah untuk ditemukan. Melalui proses forensic, security experts menganalisa virus dan membentuk respon closed-loop tertentu.

Bab 2 Panduan Konfigurasi

2.1 Endpoint Secure terhubung ke Cyber Command

1. Klik **New** untuk menambahkan perangkat Endpoint Secure baru pada Cyber Command (Alamat konfigurasi: **System -> Correlated Devices -> Correlated Devices**), masukan Device IP, Device Name, Port, otentikasi akun dan kata sandi (jika otentikasi tidak dikonfigurasi, perangkat akan secara otomatis membuatnya), seperti ditampilkan dibawah ini:

The screenshot shows a 'New' configuration window with the following fields and options:

- * Device IP:** 192.168.1.39
- * Device Name:** Sangfor Endpoint Secure
- Type:**
 - ☐ Internet Access Management
 - ☒ Endpoint Secure
 - ☐ SSL VPN
 - ☐ Wireless Access Controller
 - ☐ Branch Business Center
- Port:** 443
- Remarks:** (empty text area)
- Advanced** (dropdown menu)
- Buttons:** OK, Cancel

A yellow information box contains the following text: "STA, NGAF, FTA, Visioner, and Host Security can be connected without being configured on Cyber Command. Connecting Endpoint Secure or DAS needs to enable port 7443."

2. Klik **new** untuk menambahkan perangkat Cyber Command baru pada Endpoint Secure
(Alamat konfigurasi: **System -> Correlated Devices**), masukan **Name**, **Device IP Address**

Correlate to Sangfor Device

Correlate NGAF and IAM devices to Endpoint Secure simply by entering Endpoint Secure Manager IP address on their managers respectively.

Peripheral Type : Cyber Command

[How to Connect?](#)

*Name :

CCOM DEMO

*Device IP Address :

192.168.1.88

*Local IP Address :

192.168.1.99

Remarks :

Remarks

Report Detection Logs :

☐ Enabled

Cancel

OK

and **Local IP Address**:

3. Cek Status Correlation

(1)Cyber Command (Alamat: **System -> Correlated Devices -> Correlated Devices**)

Correlated Devices

Refresh

Total Logs (today): 0 | 5 Sangfor devices licensed, 5 licenses remaining (not count in STA, file reputation & threat analytics system)

Endpoint Secure
Online: 3 Offline: 0
Today's Synced Logs: 0

STA
Online: 1 Offline: 0
Today's Synced Logs: 0

IAM
Connected: 1 Offline: 0
N/A (sync not supported)

+ New | X Delete | Refresh

199

No.	Name (IP Address)	Type	IP Address	Version	Licensed	Sync Mode	Today's Synced Logs	Total Synced Logs	Today's Log Entries	Last Synced	Status
199 is found in 1 entries Cancel											
1	Sangfor Endpoint ...	Endpoint Se...	192.168.1.99	3.2.2	Licenses Used	Detailed View	3.52KB	3.52KB	-	2020-12-16 16:06:40	Normal

(2)Endpoint Secure (Alamat: **System -> Correlated Devices**)

Correlated Devices

[Learn About Security Integration](#) | [How to Connect?](#)

NGAF
Connected : 0

Cyber Command
Connected : 1

IAM
Connected : 0

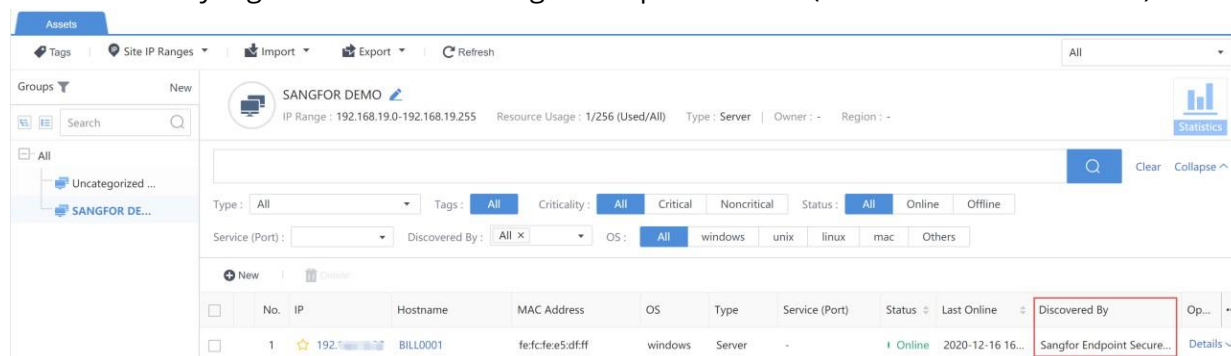
Platform-X
Connected : 0

+ New | Refresh

Device Type | Time Connected | Last Correlated | Device name, IP address:

No.	Device Name	Device Type	Device IP	Version	Log Reporting	Remarks	Time Connected	Last Correlated	Operation
1	Sangfor CCOM	Cyber Command	192.168.1.88	3.0.48	ON	-	2020-12-16 15:55:...	2020-12-16 16:01:40	Test Connectivity Delete

4. Berikut aset yang ditemukan oleh Sangfor Endpoint Secure (Alamat: **Assets -> Assets**).



No.	IP	Hostname	MAC Address	OS	Type	Service (Port)	Status	Last Online	Discovered By	Op...
1	192.168.19.0-192.168.19.255	BILL0001	fe1cfe:e5:dfff	windows	Server	-	Online	2020-12-16 16...	Sangfor Endpoint Secure...	Details

2.2 Correlated Block

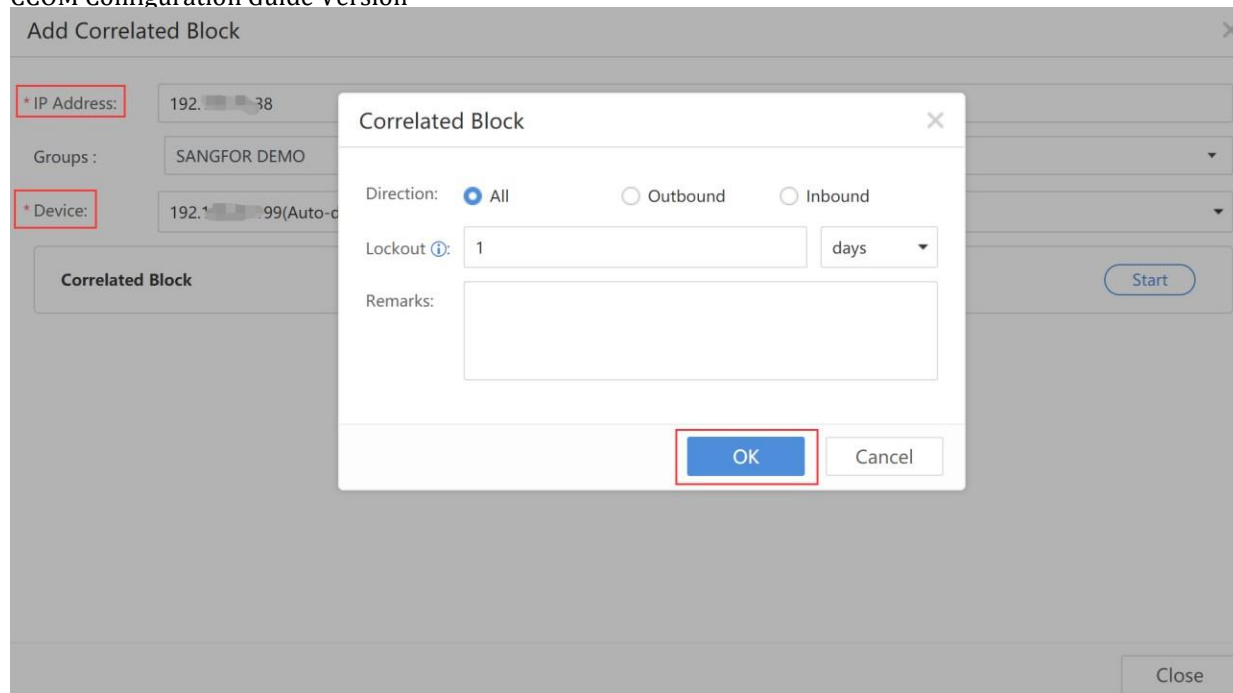
Q: Apa itu correlated block?

A: Correlated block digunakan untuk memblokir akses ke atau dari endpoint dengan alamat IP tertentu.

Q: Dalam skenario yang mana saya harus menggunakan correlated block?

A: Anda dapat correlate Endpoint Secure untuk mengisolasi atau memblokir sebuah endpoint ketika perihai keamanan terdeteksi. contoh, jika perihai keamanan terdeteksi pada sebuah endpoint, Sangfor Endpoint Secure akan berkolerasi untuk mengisolasi dan memblokir endpoint yang dimaksud, untuk menghindarinya dari membahayakan endpoint lainnya pada jaringan.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Correlated Block**. Klik **New** untuk menambah Correlated Block Policy.



【IP Address】 Alamat IP address endpoint.

【Device】 Perangkat Sangfor Endpoint Secure.

【Direction】 Arah Traffic.

【Lockout】 Atur jarak waktu yang mana endpoint perlu di blokir.

2.3 Access Control

Q: Apa itu access control?

A: Access control hampir sama dengan correlated block, tapi access control dapat memblokir akses keluar masuk ke endpoint pada semua port tertentu, membuatnya lebih rinci daripada correlated block.

Q: Kenapa saya harus menggunakan access control?

A: Access control dapat mencegah ancaman keamanan, dan ketika ancaman keamanan terdeteksi, kalian dapat dengan cepat memblokir akses endpoint tanpa mempengaruhi operasi sistem bisnis

New untuk menambahkan Access Control Policy. Access Control policy dapat membatasi IP

Access Control



* Direction: ☒ Outbound

* DstIP:

One IP address or range per row

192.168.1.1

192.168.1.0/24

192.168.1.0/255.255.255.0

192.168.1.0-192.168.1.255

Port:

☒ Custom

Enter port/port range, separate them by comma

☐ All

Period ⓘ:

1

days ▼

+ New

☐ Inbound

dan port.

2.4 Threat Scan

Q: Apa itu threat scan?

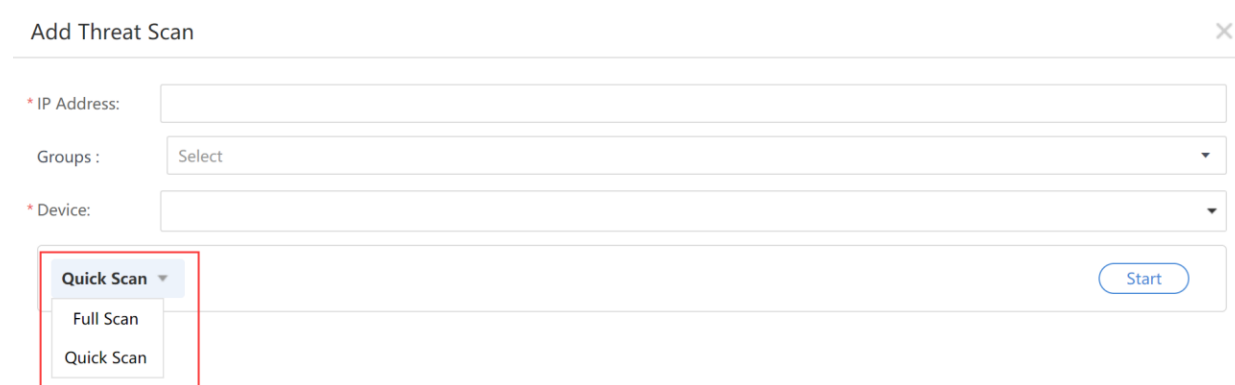
A: Threat scan mengacu pada melakukan full scan atau quick scan pada endpoint yang beresiko. Jika berkas virus terdeteksi, tindakan dapat langsung diambil.

Q: Bagaimana saya melakukan threat scan?

A: Jika sebuah endpoint terinfeksi, correlate Endpoint Secure akan melakukan virus scan dan membuang berkas yang terinfeksi.

Ketika correlated, jika virus apapun terdeteksi pada sebuah endpoint, Endpoint Secure merespon option akan tersedia langsung pada Cyber Command, jadi virus-virus dapat dibuang dengan cepat dan dengan mudah tanpa harus masuk ke Endpoint Secure Manager.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Threat Scan**. Klik **New** untuk menambahkan Threat Scan Policy. Kita dapat secara manual mengatur scan



The screenshot shows the 'Add Threat Scan' configuration window. It includes fields for IP Address, Groups, and Device. A dropdown menu for scan mode is highlighted with a red box, showing options for 'Full Scan' and 'Quick Scan'. A 'Start' button is visible to the right of the dropdown.

mode ke Full Scan atau Quick Scan.

2.5 Forensics

Q: Apa itu forensics?

A: Forensics mengacu pada proses mengumpulkan bukti yang mana endpoint beresiko mengunjungi botnet domain yang berbahaya. Bukti termasuk nama, detail proses, dsb.

Q: Bagaimana saya melakukan forensics?

A: Jika sebuah endpoint terinfeksi, correlate Endpoint Secure akan melakukan virus scan dan menghapus file terinfeksi.

Forensics secara khusus berguna ketika berkas virus susah untuk ditemukan. Melalui proses forensics, security experts mengalisa virus dan membentuk respon closed-loop tertentu.

Pergi ke **More->Toolkit->Correlated Response->Endpoint Secure->Forensics**. Klik **New** untuk menambahkan Forensics policy.

Add Forensics

* IP Address:

192.168.1.38

Groups :

SANGFOR DEMO

* Device:

192.168.1.38 (Auto-discovered)

Forensics

Start



Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc